1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: (updated) December 4, 2012

(b) Name of system: Passport Lookout Tracking System

(c) System acronym: PLOTS

(d) IT Asset Baseline (ITAB) Number: 346

(e) System description (Briefly describe scope, purpose, and major functions):

The Passport Lookout Tracking System (PLOTS) is a web enabled case management and image archive system used to manage and adjudicate Consular Lookout Automated Support System (CLASS) cases. The purpose of the PLOTS application is to provide an efficient and reliable solution to the recording, managing, searching and process streamlining needs of domestic Department users, posts, and external agencies entering CLASS lookouts associated with a PLOTS lookout record locally.

(f) Reason for performing PIA:

[ ] New system

[ ] Significant modification to an existing system

[X] To update existing PIA for a triennial security re-certification

(g) Explanation of modification (if applicable):
N/A

(h) Date of previous PIA (if applicable): August 21, 2008

3. Characterization of the Information

The system;

[ ] does NOT contain PII. If this is the case, you must only complete Section 13.

[X] does contain PII. If this is the case, you must complete the entire template.

a. What elements of Pll are collected and maintained by the system? What are the sources of the information?

PLOTS collects and maintains records related to applications for U.S. passports. PLOTS does not maintain evidence of travel such as entrance/exit stamps, visas, or residence permits. Such information is entered into the passport after it is issued. Sources of the information are U.S.

citizens applying for passports, other Department of State computer systems, passport specialists, and fraud prevention managers.

The record subjects in PLOTS are applicants for a U.S. passport who are suspected of having felony warrants or of committing passport fraud, who owe debts to dependents or to the federal government, or who may be denied a passport or be issued only a restricted passport for certain other reasons permissible by statute.

Components of an individual's record (called a "case") in PLOTS are of two kinds. The first kind is the passport application and all supporting documentation related to it, including citizenship evidence, correspondence, reports of investigation, passport specialists' diary entries, court orders, passport revocation actions, and passport denial actions. (For a detailed description of PII in passport applications, please see the TDIS PIA.) The passport application and supporting documents are imported into PLOTS electronically by way of separate Consular Affairs passport processing systems, not directly from the applicant.

The second kind of information in PLOTS about an individual is one or more "lookouts." Lookouts serve to alert passport specialists of possible fraud or other irregularities related to a person having the same or similar name and date of birth as that of the applicant. Lookouts may be created by passport specialists at passport agencies/centers and at overseas posts using a separate Consular Affairs computer system called the Consular Lookout and Support System (CLASS), or may be created directly in PLOTS by the specialist.

b. How is the information collected?

Passport applicant information is imported into PLOTS. Information is collected directly from the passport application on any of the following forms:

- Form DS-11 is used for passport applications from first time applicants, persons replacing a lost or stolen passport, all applicants under the age of 16, and in cases where the previous passport was issued more than 15 years earlier.
- Form DS-82 is for persons applying to replace a passport issued within the past 15 years and who also provide the old passport with the application form.
- Form DS-5504 is for persons replacing a passport that was issued less than a year earlier. The form may be used to replace an emergency passport with a full validity one; to make a change to the applicant's identifying information (e.g., name change due to marriage or court order); or to correct a printing error in their passport.
- Form DS-4085 is used to add visa pages to a previously issued and currently valid passport

The above forms may be completed by the applicant on published paper forms available at many government office locations or may be completed online using web forms at the Department of State's public web site. If web forms are used, the applicant must still print the form and submit it as hardcopy with supporting documents.

Lookouts and diary entries (described above) are key-entered into the PLOTS case file by fraud prevention mangers and passport specialists by using PLOTS directly or by an indirect feed from CLASS. The CLASS system performs name checks on U.S passport applications to identify those who are ineligible or require special action. PLOTS enables internal users to easily search, add, and delete Lookout records to and from the Consular Lookout and Support System (CLASS).

c. Why is the information collected and maintained?

The U.S. passport identifies the bearer as a U.S. citizen or national. It is a request to foreign governments to permit travel or temporary residence in their territories and access to all lawful local aid and protection. It also allows bearers access to U.S. consular services and assistance while abroad and re-entry into the U.S.

PLOTS collects and maintains only information that is directly relevant to the lawful issuance of passports and the protection of the integrity of the passport as proof of United States citizenship at home and around the world. Information collected and maintained in PLOTS is used only for those purposes.

PLOTS warns passport agency officials that an applicant may, by statute or regulation, be ineligible to receive a passport or that a passport should have restrictions put upon it. PLOTS is used by domestic and overseas Department of State staff. PLOTS provides fraud prevention managers and passport specialists with the ability to view all information related to the applicant's case, including information that originates in other Consular Affairs systems.

PLOTS permits fraud prevention managers and passport specialists from one passport agency to examine possible fraud attempts at other passport agencies. For example, if an individual were indicated in a fraudulent attempt to obtain a passport in Boston and he or she makes a subsequent attempt with the same name or identification in New York, New York staff are able to examine the materials and digital images of the previous attempt in Boston.

d. How will the information be checked for accuracy?

Accuracy of the information on a passport application and supporting citizenship evidence is the responsibility of the passport applicant. When applicants prepare their application using an available online web form, the application bears a computer-readable bar code.

The code permits machine-readable entry of their information into a separate Consular Affairs computer system called Travel Document Issuance System (TDIS) without repeat key entry by Consular Affairs staff. This feature helps to minimize transcription errors.

Quality control measures based on layered approvals ensure that lookouts and other information (e.g., diary entries) entered in the case file by passport specialists are accurate and relevant to the record subject and minimize instances of faulty adverse determinations.

No technology or capability exists in the system to identify, monitor, track, or locate individuals in "real time." Address and contact information of passport applicants is collected on their application or supporting documents. The information may reflect locations where the individual has interacted with a passport agency or center. Address and contact information is used only to contact or correspond with the applicant regarding their case, or by law enforcement under the authority of a routine use described in Privacy Act system of records named STATE-26, Passport Records.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 8 U.S.C. 1401–1503 (2007) (Acquisition and Loss of U.S. Citizenship or U.S. Nationality; Use of U.S. Passports)
- 18 U.S.C. 911, 1001, 1541–1546 (2007) (Crimes and Criminal Procedure)
- 22 U.S.C. 211a–218, 2651a, 2705

- Executive Order 11295 (August 5, 1966), 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 8 U.S.C. 1185 (Travel Control of Citizens)
- 8 U.S.C. 1202(f) (Confidential Nature of Visa Records)
- 22 U.S.C 2651(a) (Organization of Department of State)
- Immigration Act of 1990 (P.L. 101-649)
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (P.L. 104-208)
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208)
- Legal Immigration Family Equity "LIFE" Act (P.L. 106-553)
- USA PATRIOT Act of 2001 (P. L. 107-56)
- Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173)

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The collection of PII in PLOTS creates the vulnerability that Department of State employees may use the PII for purposes other than those required by the Department of State and thereby misuse the PII. The potential threats to privacy include:

- Inadequate security by the Department of State — Department of State employees may create a new repository of PII that is vulnerable to unauthorized access, use, disclosure and retention;
- Inadequate data integrity — Department of State data entry personnel may enter the data into PLOTS incorrectly and may modify the data without authorization.
- Unauthorized access – Department of State employees may view record to which they do not have a business need to access.

The Department of State seeks to address these risks by limiting the collection and transmission of PII to the information required to execute these processes. Moreover, only authorized users with a need to know are granted access to PLOTS.

4. Uses of the Information

a. Describe all uses of the information.

PLOTS collects and maintains only information that is directly relevant to the lawful issuance of passports. In some circumstances, an individual's case record may be associated with one or more "entities" in PLOTS. An entity can be another person, business, institution, or an organized crime ring, and is defined as a set of cases having certain common characteristics. An entity allows a passport specialist to establish a connection between one case in PLOTS with other case record subjects. For example, a case may be associated with a particular travel agency where passport applicants conduct business, or may be associated with an address or neighborhood. A case may be included in more than one entity. The only determinations made about the individual applicant based on their association with an entity (or entities) relate to eligibility for passport issuance, which is the statutory purpose for all information maintained in PLOTS.

An individual's record is retrieved from PLOTS by their name, mother's maiden name, Social Security number, passport application number, date of birth, and place of birth. Because records are retrieved by name and/or other unique identifiers, PLOTS constitutes a Privacy Act system of records.

No technology or capability exists in the system to identify, monitor, track, or locate individuals in "real time." Address and contact information of passport applicants is collected on their application or supporting documents. The information may reflect locations where the individual has interacted with a passport agency or center. Address and contact information is used only to contact or correspond with the applicant regarding their case, or by law enforcement under the authority of a routine use described in Privacy Act system of records named STATE-26, Passport Records.

b. What types of methods are used to analyze the data? What new information may be produced?

New information produced by PLOTS is lookouts, diary entries, and associations of the case to entities. Lookouts and entities are terms described above. PLOTS and the personal information collected and maintained by PLOTS are not an ingredient in any "data mining activity" as defined by federal law.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

PLOTS does not use commercial information, publicly available information, or information from other Federal agency databases.

d. Is the system a contractor used and owned system?

PLOTS is a government system. It is supported by contract employees, some of whom are located at contractor-owned facilities. Direct-hire U.S. government employees have the sole responsibility for adjudicating passport applications in PLOTS to determine if applicants are U.S. citizens and qualify for passport issuance. Contractors do support government employees with regard to other Consular Affairs computer systems by entering data, printing and mailing passports, and answering customer service inquiries.

Contractors involved in the passport fulfillment process (i.e., data entry, scanning, or correction of records or the printing and mailing of passports) are subjected to a background investigation by the contract employer equivalent to a "National Agency Check" of the files of certain government agencies (e.g., criminal law enforcement and homeland security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual. All contractors involved in the development or maintenance of PLOTS hardware or software must have at least a Secret-level security clearance.

All contract employees undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved

Federal Acquisition Regulation (FAR) Privacy Act clauses. Contractor-owned facilities are periodically inspected by Consular Affairs.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

PLOTS has heightened privacy risk because it creates new information about a record subject based on information from sources other than the passport applicant. Most determinations in PLOTS are triggered by irregularities within the passport application that may indicate fraud. Since these are critical determinations that may have an adverse impact on the passport applicant, PLOTS users are specifically trained to preserve data accuracy and integrity and to avoid faulty determinations or false inferences about the record subject, thereby mitigating privacy risk. There

is also no risk of "function creep," wherein with the passage of time PII is used for purposes for which the public was not given notice. Based on these specific safeguards, there are adequate protections to decrease the likelihood of improper use or adverse determinations about the record subject.

To protect the data there are numerous management, operational, internal, and technical security controls implemented in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the information assurance standards published by the National Institute of Standards and Technology (NIST). These controls include regular security assessments, physical and environmental security, encryption, role-based access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), annual training and audit reports.

5. Retention

a. How long is information retained?

By law, the retention period for passport records is 100 years and applies to information in the system such as the passport application and supporting documents. A PLOTS case may be closed when it is determined to have been completely adjudicated, i.e., passport issuance, restricted issuance, or denial of the passport. Closed cases remain in the system as archived records subject to the record schedule for passport records. (A-13-001-16 and A-13-001-17)

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

The privacy risk from retention of information is minimal. A retention schedule tailored to the needs of the system and the rights of the record subjects is in place, as well as internal safeguards that are designed to protect the information. The utility of the information in the system about a particular individual will not extend over the allotted time in the Department of State's Disposition of Schedule, as defined in Chapter 13 Passport Records. All PII in the database has the same access restrictions and controls as production data. Moreover, there is negligible privacy risk as a result of degradation of its information quality over an extended period of time.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

The Bureau of Consular Affairs oversees a network of facilities that may internally share or disclose the personal information collected and maintained in PLOTS. These facilities include over a dozen regional passport agencies, a special issuance agency, four national Processing facilities, the National Passport Information Center, and the Headquarters offices in Washington, DC. United States embassies and consulates abroad may also be involved in the adjudication of a PLOTS case. Information is shared within these entities only for the purpose of issuing or denying a passport, subject to the law.

Within State, only internal users can access PLOTS information within the Consular Consolidated Database (CCD). Access to PLOTS data in CCD is restricted to only users with the properly defined

role and a need to know and a rationale must be approved via a dialog box for accessing specific information. All access is audited and monitored within the CCD.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

PLOTS obtains information from CLASS, PRISM and TDIS for its purposes by first sending one XML query to the Front End Processor (FEP). FEP then sends out queries to the appropriate systems (CLASS, PRISM and/or TDIS). The responses come back to FEP; FEP consolidates them (if appropriate) and returns the comprehensive query results to PLOTS.

PLOTS shares information in two ways. When cases are referred to DS the data is pushed to the DS system. However, when case status is requested, this is done in a query/response fashion. All transactions happen between PLOTS and the DS-IMS system by sending XML via a SOAP service call to the receiving DS system. The DS system responds per an established Interface Control Document to the Windows SOAP service and that service turns around and writes to the PLOTS database.

In either case PLOTS does not use SSL/TLS for protection in transit to DS or FEP since the transmission remains within the OpenNet network. To FEP, FEP uses IP filtering as its means of authentication. Between PLOTS and DS/IMS – uses username/password authentication.

The query to FEP is on demand. The push of data to DS-IMS and the query for Field offices is on demand; however, the query for case status is every hour.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

Internal sharing occurs only with authorized users, who are cleared government employees or contractors with work-related responsibilities specific to the access and use of the information. No other internal disclosures of the information within the Department of State are made.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

External agencies can only provide names to be included in the PLOTS database; however, this one-way transaction is not accomplished through access to PLOTS by external agencies; external users can only access CCD. CCD replicates the names to PLOTS on behalf of the user.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Information from PLOTS is not shared externally; PLOTS only receives names from external organizations through CCD.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

The risks associated with sharing privacy information externally and the disclosure of privacy information is generally higher than internal sharing and disclosure. Intentional and unintentional

disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. Transmission of privacy data in an unencrypted form (plain text), and use of non-secure connections are also a serious threat to external sharing. Numerous management, operational, and technical controls are in place to reduce and mitigate the risks associated with external sharing and disclosure including, but not limited to formal Memorandums of Agreement/Understandings (MOA/MOU), service level agreements (SLA), annual security training, separation of duties, least privilege and personnel screening.

8. Notice

The system:

[X] constitutes a system of records covered by the Privacy Act.
STATE-26, Passport Records

[ ] does not constitute a system of records covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

An individual can decline to submit the information, and will not receive a passport. However as PLOTS does not collect the information directly from the individual, individuals who apply for a passport have no opportunity and/or right to decline the inclusion of their information in PLOTS.

The passport application collects the information from the individuals, and provides a Privacy Act Statement containing the authorities for collection of the information solicited on the form, purpose for soliciting the information, routine uses of the information solicited on the form and consequences of failure to provide information.

Also, notice is provided in the System of Records Notice (SORN) Passport Records, State-26.

b. Do individuals have the opportunity and/or right to decline to provide information?

Application for a passport is a voluntary action by a record subject. No provision exists within the law for an applicant to decline to provide part or all the information required on the passport application form.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Information collected on the passport application form is used for the sole purpose of processing the application in accordance with law. Limited, special, and/or specific uses of the information do not apply to this programmatic need.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

Notice is provided to the individuals on the forms used to submit a passport application. Additionally the Department published a System of Records Notice (SORN), State-26, Passport Records, which provides notice to the public of the uses of the information. While

PLOTS does not provide direct notification, it is mitigated by the notice at time of collection, and the publication of the SORN.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

PLOTS contains Privacy Act-covered records; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the system of records notice identified in paragraph 8 above, and in rules published at 22 CFR 171.30. The procedures inform the individual about how to inquire about the existence of records about them, how to request access to their records, and how to request amendment of their record. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of a passport record on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.36.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purposes and uses and its applicable legal requirements, thus there are no risks associated with notification and redress.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Access to PLOTS is limited to authorized Department of State staff having a need for the system in the performance of their official duties. All authorized government users maintain a security clearance level at least commensurate with public trust positions. To access the system, the individual must first be an authorized user of the Department's unclassified computer network. Access to the network requires a unique user name and password assigned by Diplomatic Security.

Each prospective authorized user must first sign a user access agreement before being given a user account. The individual's supervisor must sign the agreement certifying that access is needed for the performance of official duties. The user access agreement includes a rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g., curiosity browsing). Completed applications are also reviewed and approved by the information system security officer (ISSO) prior to assigning the logon.

The level of access for the user restricts the data that may be seen and the degree to which data may be modified. A system use notification ("warning banner") is displayed before log-on is permitted and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

Non-production uses (e.g., testing, training) of production data are limited by administrative controls.

b. What privacy orientation or training for the system is provided authorized users?

All users are required to undergo computer security and privacy awareness training prior to accessing the system, and must complete refresher training yearly in order to retain access.

c. Privacy Impact Analysis: Given the sensitivity of Pll in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

No such residual risk is anticipated. Moreover, several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a particular user performed--or attempted to perform--on an information system.)

11. Technologies

a. What technologies are used in the system that involves privacy risk?

PLOTS operates under standard, commercially-available software products residing on a government-operated computing platform not shared by other business applications or technologies. No technologies commonly considered to elevate privacy risk are employed in PLOTS.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

The system does not use any technologies that are considered to cause privacy risk.

12. Security

What is the security certification and accreditation (C&A) status of the system?

The Department of State operates the system in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls. The Department performs monitoring, testing, and evaluation of security controls on a regular basis to ensure that the controls continue to work properly.

In accordance with the Federal Information Security Management Act, PLOTS was certified and accredited in May 2010. This authority to operate is valid until May 2013.